学校编码：10384　　分类号＿＿密级＿＿＿＿
学号：23120070153488　　UDC ＿＿＿＿＿＿＿＿

厦门大学

博　士　学　位　论　文

混沌非对称加密算法的安全性问题及其应用设计研究

The security of chaotic asymmetric encryption and its application design

李国刚

指导教师姓名：　郭东辉 教授
专　业　名　称：　电路与系统
论文提交日期：　2012 年 11 月
论文答辩日期：　2013 年 1 月

答辩委员会主席：＿＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿＿

2013 年 1 月

混沌非对称加密算法的安全性问题及其应用设计研究

李国刚

指导教师 郭东辉 教授

厦门大学

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

20　年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

20　　年　　月　　日

摘 要

自从 1976 年 W.Diffie 和 M.Hellman 首次提出了公钥密码系统，它便成了现代密码学的焦点。传统公钥算法由于量子算法的出现而受到威胁，急需研究新型公钥算法。离散 Hopfield 神经网络的非线性动力学特性，特别其混沌动力学特性，可视为复杂难解的 NP 问题。此外，离散 Hopfield 神经网络是也一种可实现高速并行运算的网络，适合用 FPGA 或 CMOS 数字集成电路来直接兑现它的并行运算，以实现实时高速传输，满足现代网络通信的实际要求。本论文针对基于 OHNN（Overstoraged Hopfield Neural Network）的公钥密码体制进行系统研究，完成单向陷门函数的数学证明，并利用可证明安全的思想指导实用的公钥密码算法设计和实现。本论文的主要研究内容和结果如下：

(1) 通过对刘年生和郭东辉等人提出的 OHNN 公钥加密系统的深入研究，根据广义逆矩阵在矩阵方程的应用，从数学理论上证明了神经元联接突触矩阵变换函数为单向陷门函数，为构建可证明安全的公钥算法打下很好的基础。(2)无线移动通信中的安全保密问题越来越受到重视，考虑到在各种移动终端上的硬件资源有限，计算能力较弱且存储容量偏小，我们设计了适合此种环境的新型流密码。算法使用线性反馈移位寄存器(LFSR)作为驱动部分，采用 OHNN 作为非线性组合部分，生成伪随机序列，并进行了相关测试。最后采用特征矩阵法，证明了此算法能够抵挡代数攻击。(3)依照混合加密的思想，设计了一种基于流密码的 OHNN 公钥密码算法，并分析了其安全性和加密效率，利用 vc 编程实现了算法。实验结果表明，本算法有较好的性能和加解密速度。同时新方案密钥空间大大增加，抗攻击能力大幅提高。(4)在 FPGA 实现了本论文公钥算法 IP 核的设计，然后将其作为密码协处理器的一部分，成功应用于 RFID 读写系统中，提高了 RFID 读写系统的安全性和加解密速度。

在文章最后，我们对全文的研究工作作了总结，并对基于混沌神经网络的公钥密码体制进一步的研究工作进行了展望。

关键词：混沌；单向陷门函数；混沌吸引子；混合公钥算法；可证明安全性

Abstract

Public key cryptography system became the focus of modern cryptography since 1976. Traditional public-key algorithms was danger due to the emergence of quantum algorithms, so the research of new public key algorithm is urgent. Nonlinear dynamics characteristics of the discrete Hopfild neural network can be regarded as the NP-complete problem. Additionally discrete Hopfiled neural network is fit to parallel computing with FPGA or CMOS digital integrated circuits. It can meet the requirements of the high-speed encrypted communication. This thesis focused on public-key cryptosystem based Overstoraged Hopfield Neural Network system. The new hybrid public key cryptography algorithm based on OHNN was designed since the one-wayness of trapdoor function was proved. The main contents of this paper and the results are as follows：

(1) Through the study of the OHNN public key encryption system proposed by LIU Nian-sheng and GUO Dong-hui et al., we proved the the one-wayness of trapdoor function according to the theory of generalized inverse matrix. The proof lay a good foundation for building provably secure public key algorithm. (2) Security in wireless mobile communication is paid more and more attention, taking into account the limited hardware resources on a variety of mobile terminals and less computing power and small storage capacity , we have designed a new stream for such environments. The algorithm uses a linear feedback shift register as a driving part and OHNN as nonlinear combining section to generate a pseudo-random sequence, and the stream was tested. Finally we proved that this algorithm is able to resist algebraic attacks using the characteristic matrix method. (3) In accordance with the idea of hybrid encryption, we design a Diffie-Hellman public key cryptographic algorithm based on OHNN. Experimental results show that the algorithm has a better performance and processing speed . Also the key space of the new algorithm and anti-attack capability greatly increased. (4) The public key algorithm was completed as IP core in the FPGA. The core improved the security and processing speed of the RFID reader system after it successfully applied to the system as part of a cryptographic coprocessor.

We have made a summary and prospect of the study work on public key cryptography based on OHNN at last.

Keywords: chaotic; one-way trapdoor function; the chaotic attractor; hybrud public-key algorithms; provable security

目 录

Table of Contents